Strategy Research Project

DEFENDING THE NEW DOMAIN: CYBERSPACE

BY

LIEUTENANT COLONEL DWIGHT R. MORGAN
United States Army

USAWC CLASS OF 2011

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 21-03-2011	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*
4. TITLE AND SUBTITLE Defending The New Domain: Cyberspace		**5a. CONTRACT NUMBER**
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Lieutenant Colonel Dwight R. Morgan		**5d. PROJECT NUMBER**
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) COL John H. Greenmyer Department of Military, Planning and Operations		**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College 122 Forbes Avenue Carlisle, PA 17013		**10. SPONSOR/MONITOR'S ACRONYM(S)**
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

For over a decade, adversaries have exploited large amounts of intellectual data from the United States through cyberspace. The United States relies on cyberspace, a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures for business transactions, government operations, and convenience. The internet has become a lucrative place for cyber spies, and criminals, who can conduct activities with speed, anonymity, and very little oversight by law enforcement. Determining whether terrorist, criminal, or state supported actors conducted the intrusion is difficult to discern without further analysis of the intrusion, which can take months. This paper reviews cyber organizations, technology, democracy, and law enforcement to determine if the 2003 document laid the groundwork to enable Americans to defend and prevent intrusions in United States cyberspace.

15. SUBJECT TERMS
USCYBERCOM, FBI, DHS, DTN, TCP/IP

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	28	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

DEFENDING THE NEW DOMAIN: CYBERSPACE

by

Lieutenant Colonel Dwight R. Morgan
United States Army

Colonel John Greenmyer
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR:	Lieutenant Colonel Dwight R. Morgan
TITLE:	Defending The New Domain: Cyberspace
FORMAT:	Strategy Research Project
DATE:	21 March 2011 WORD COUNT: 5,426 PAGES: 27
KEY TERMS:	USCYBERCOM, FBI, DHS, DTN, TCP/IP
CLASSIFICATION:	Unclassified

For over a decade, adversaries have exploited large amounts of intellectual data from the United States through cyberspace. The United States relies on cyberspace, a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures for business transactions, government operations, and convenience. The internet has become a lucrative place for cyber spies, and criminals, who can conduct activities with speed, anonymity, and very little oversight by law enforcement. Determining whether terrorist, criminal, or state supported actors conducted the intrusion is difficult to discern without further analysis of the intrusion, which can take months. This paper reviews cyber organizations, technology, democracy, and law enforcement to determine if the 2003 document laid the groundwork to enable Americans to defend and prevent intrusions in United States cyberspace.

DEFENDING THE NEW DOMAIN: CYBERSPACE

For over a decade, adversaries have exploited large amounts of intellectual data from the United States through cyberspace. The United States relies on cyberspace, a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures for business transactions, government operations, and convenience. The internet has become a lucrative place for cyber spies, and criminals, who can conduct activities with speed, anonymity, and very little oversight by law enforcement. Determining whether terrorist, criminal, or state supported actors conducted the intrusion is difficult to discern without further analysis of the intrusion, which can take months.

In the late 1990s, the United States discovered a series of intrusions conducted by Russians and named the intrusion Titan Rain. In the early 2000s, the United States found another set of intrusions, this time by the Chinese, and named the intrusions Mystic Farm. To combat these intrusions, the Department of Defense (DoD) stood up Joint Task Force Global Network Operations (JTF-GNO) in 1999 and Joint Forces Component Command Network Warfare (JFCC-NW) in 2002 to conduct Network Operations (NetOps), defense operations, and attack operations to defend and prevent intrusions on military networks.

In February 2003, President Bush published the National Strategy to Secure Cyberspace. The purpose of the document is to secure cyberspace but the intent was for the private sector to defend and prevent cyber attacks on the part of the network that they own and operate. All networks, to include the DoD information network and government networks, depend on the civilian backbone networks. The National Strategy to Secure Cyberspace encourages Americans to collaborate with each other and the government to develop organizations to defend U.S. cyberspace. This paper reviews cyber organizations, technology, democracy, and law enforcement to determine if the 2003 document laid the groundwork to enable Americans to defend and prevent intrusions in United States cyberspace.

Department of Homeland Security

President Bush signed legislation creating the Department of Homeland Security (DHS) in November 2002.[1] This legislation and the Homeland Security Presidential Directive (HSPD) -7 appointed DHS as the focal point for the security of U.S. cyberspace.

> DHS executes the mission of protecting U.S. government and private networks by: (1) Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States, (2) Providing crisis management in response to attacks on critical information systems, (3) Providing technical assistance to private sector and other government entities with respect to emergency recovery plans for failures of critical information systems, (4) Coordinating with other agencies of the federal government to provide specific warning information and advice about appropriate protective measures and countermeasures, (5) Performing and funding research and development along with other agencies that will lead to new scientific understanding and technologies in support of homeland security. Implementation of this policy shall include a voluntary public-private partnership, involving corporate and nongovernmental organizations.[2]

Under Homeland Security Presidential Directive (HSPD) -7, DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance critical infrastructure and key resources protection.[3] Critical infrastructure and key resources are those physical and cyber based systems so vital to the United States that their incapacity or destruction would have a debilitating effect on security, economic security, national public health, and safety. Critical infrastructure and key resources are banking and financing, chemical plants, emergency services, agriculture and food processes, electric grid and energy systems, telecommunications, postal and shipping, public health services and the water supply.

Following President Bush's guidance in the National Strategy to Secure Cyberspace, DHS implemented the National Infrastructure Protection Plan (NIPP). The NIPP's goal is to prevent, deter and mitigate the effects of deliberate efforts by adversaries to exploit or destroy elements of the critical infrastructure.[4] As the lead agency for information technology sector, DHS formally chartered the Information Technology (IT) Sector Coordinating Council in January 2006. The council consists of private companies, as well as the IT Information Sharing and Analysis Center (IT-ISAC).

Although DHS has the responsibility to protect and defend government and private sector networks, DoD has the responsibility to conduct military operations to defend cyberspace and critical infrastructures.[5] Traditional or conventional command and control structures will not enable DHS to collaborate with DoD fast enough for DoD and DHS, to react to incidents, to defend U.S. networks and critical infrastructure. The current command and control structure does not allow DHS or DoD to collaborate and share information at the speed of light, because DHS and DoD have separate common operational pictures. These organizations need to reassess their command and control approach, organization, systems, and technology in order to discover and gain situational awareness of intrusions as they occur. Until the United States uses technology, processes, and standards to operate at the speed of networks, the United States will always react to incidents rather that actively prevent them.

Technology

Inexpensive technology allows criminals, spies, and hackers a way to attack America without the need to defeat America's air or land forces. Adversaries have taken advantage of the gaps in security on the internet to steal intellectual property, hold companies for ransom and gain access to personal information for monetary gain. China and Russia have developed offensive capabilities that have exploited U.S. networks. In 1998, cyber attacks code named Moonlight Maze appeared to have come from Russia; however, Russians officials denied any knowledge of the attacks. The attacks lasted for approximately three years.[6] In May 2001, a denial of service attack defaced and disabled the White House web site for three hours. The attack originated from Internet Protocol (IP) addresses located in China. Attacks originating from IP addresses in other countries have occurred since the 1990s. Today, intrusions are so sophisticated that organizations discover the intrusion days to months after the intrusion happened.

There are many advances transpiring in technology and different ways that we use the technology, such as smart phones and social websites like Facebook. The main purpose of these devices and applications is to share information and allow many people to have access to information anytime and anywhere. Security is secondary to ensuring a device, an application or software sends or receives information. Adversaries take advantage of new software applications because so often they have vulnerabilities not identified during creation. New Microsoft Operating Systems have unknown vulnerabilities after initial release, which is the reason they often have security packs and monthly updates.

DoD is taking advantage of social websites and other devices to share information and to make some tasks more efficient. The United States Army is researching a program to give smartphones and tablets to soldiers for use in garrison and the field to send and receive information. Smartphones and tablets will assist the soldier with training, assist the soldier with administrative functions and the smartphone will track friendly forces in a field environment.

The private sector is taking advantage of cyberspace by using social media websites, smartphones, and applications to control or execute processes. Applications used over cyberspace are allowing private citizens to control the heat in their house, record television programs and start their car. Bank customers are conducting transactions online at their convenience and in minutes rather than taking a half-hour or longer to go to a bank and stand in line. With the U.S. becoming ever more dependent on cyberspace for business applications, control of processes and private sector convenience, there is a need to make cyberspace secure. The United States and its allies must start building networks and applications built with security as a foundation of the new technology.

For the last several years, the government has been developing a plan to employ and use Internet Protocol version 6 (IPv6) on DoD networks. The U.S. Department of Defense announced that it would transition to IPv6, citing the requirement for end-to-end security, as well as more addresses for military combat applications. Many professionals believed IPv6 was inherently more secure than IPv4 of the separate network layer protocol, IPSec. Although this may be true in an ideal environment with well-coded applications, a robust identity infrastructure, and efficient key management, in reality the same problems that plague IPv4 Internet Protocol Security (IPsec) deployment will affect IPv6 IPsec deployment.[7]

This is true for a number of reasons. IPv6 will also suffer other security issues because many of the security breaches occur at the application level of the Open Systems Interconnection (OSI) model. IPv6 will be vulnerable to scans, unauthorized access, network and transport spoofing, routing attacks, viruses and worms. Hacker will try to gain unauthorized access by establishing connectivity in the upper layer protocols and applications by exploiting the open transport layer policy. Adversaries will still have the ability to spoof their IP addresses. Adversaries will be able to modify their source IP address to hide their location and deceive those trying to locate the origin of an attack. IPv6 will not prevent adversaries from executing denial of service attacks; adversaries will spoof source address and send out requests to multiple computers. These computers will reply, flood the source address, and prevent that computer or server from communicating with any other computer. Viruses and worms remain one of the most significant problems in IP networking today and they remain a problem with IPv6.

IPv6 is a network centric protocol, just as IPv4 is; therefore, some of the same vulnerabilities will cause security issues. New vulnerabilities not identified yet will also cause some security issues for IPv6. IPv4 and IPv6 are inherently unsecure protocols, and this is why the U.S. needs to move from these unsecure protocols to a new network; a network with different protocols that include security throughout the development of the protocol.

To address the concerns of the network centric networks, Defense Advanced Research Projects Agency (DARPA) is developing an innovative network, Disruption Tolerant Network (DTN), which will dramatically alter the cyber defense landscape. DTN is a set of protocols designed to replace the legacy Transmission Control Protocol/Internet Protocol (TCP/IP) suite.[8] DoD designed TCP/IP in the 1970s to move data from one point to another with no thought of security. DARPA built DTN based on a data-centric model versus the TCP/IP model, which is a network-centric model. DTN addresses major concerns with the legacy IP networks that are nearly impossible to secure fully.[9] Moreover, DTN will provide a reliable and robust network for mobile ad hoc networks used in military tactical domains. Cyber defense has challenged DoD networks for years and traditional methods of reacting to known cyber attacks are not working. As a result, DTN is a growing project within DARPA to dislodge the DoD network from the legacy TCP/IP architecture; however, this change is still many years from being reality.

The government and the private sector must continue to look at new technology such as quantum computing. Although quantum computing is not practical now, it will be in the future and the U.S. does not want to be the last to operationalize this technology. In today’s computer, a bit is a fundamental unit of information, classically represented as a zero or one in your digital computer. In a quantum computer, the fundamental unit of information is call a quantum bit or qubit and it is not binary in state like our computer today.[10] The qubit can exist in a state as zero, one, or zero and one at the same time, called superposition. It is like flipping a coin that lands on heads and tails simultaneously. The significance of this superposition state is, in contrast to classical computers, where memory is a string of 'ones' and 'zeros', quantum bits (or qubits) can be in a superposition of many different states at once, so a quantum computer has the potential to be much more powerful than a classical computer.[11]

In November 2010, New York Times reported that IBM has reconstituted what had recently been a relatively low-level research effort in quantum computing. IBM is responding to advances made in the past year at Yale University and the University of California, Santa Barbara, that suggest the possibility of quantum computing based on standard microelectronics manufacturing technologies.[12] Creating and maintaining qubits in entangled states has been immensely challenging. However, the number of qubits is increasing slowly; the precision with which the researchers are able to control quantum interactions has increased a thousand fold.[13] Fortunately, the House of Representatives Armed Services Committee is aware of the emerging technology and has authorized the DoD to conduct research and development on quantum computers.

ECONOMIC

U.S. companies send manufacturing processes overseas to increase profits, but there are risks. One risk is the compromise of software or hardware in the production process. Government agents, hackers, or personnel working on the production of hardware and software can insert malicious code, which can cause sudden malfunctions, into software during development. The malfunctions could cause a computer to shut down or allow remote access into a computer system allowing actors to manipulate the system. The risk of compromise in the manufacturing process is very real and tampering is almost impossible to detect and even harder to eradicate.[14] The Department of Defense has detected counterfeit hardware in systems that the department has procured.[15] Some technology companies have developed technology and processes to detect malicious code but that does not prevent the adversaries from gaining access to company servers through privately owned computers that have the malicious code.

The cost of economic espionage is a major impact on the U.S. economy. The Annual Threat Assessment of the Intelligence Community estimates total cyber-related business losses in 2008 to be 42 billion dollars for the United States.[16] Malicious actors steal intellectual property many times larger than all the intellectual property contained in the Library of Congress from networks maintained by U.S. businesses, universities, and government agencies every year.[17] Criminals, hackers, and state supported actors execute crimes for extortion, ransom, intelligence, or bragging rights. The 42 billion dollars in losses for the United States is an estimate because many businesses do no report intrusions or are unaware of the intrusion.

DIPLOMACY

According to the National Strategy to Secure Cyberspace, published February 2003, the Department of State will lead the effort to enhance international cyberspace security cooperation.[18] The U.S. is dedicated to working with International organizations such as the Organization of Economic Cooperation and Development (OECD), G-8, the Asia Pacific Economic Cooperation (APEC), and the Organization of American States. The U.S. plans to work with Canada and Mexico to make cyberspace in North America secure. The U.S. goal is to share real time threat information as information becomes available through an International Watch and Warning network.[19] The U.S. signed the Council of Europe Convention on Cybercrime to demonstrate that the U.S. is collaborating with the international community to secure the internet. The U.S. is also encouraging other nations to agree or comply with the Convention on Cybercrime.

According to the National Strategy to Secure Cyberspace, the federal government states it realizes that the United States is a nation now fully dependent on cyberspace and that the federal government cannot defend U.S. cyberspace without the help of the private sector.[20] The National Strategy to Secure Cyberspace empowers the American people to secure the portions of the cyberspace they own and operate. The strategy is part of an overall objective to protect the nation. The strategic objectives are consistent with the strategy for homeland security:

- Prevent cyber attacks against America's critical infrastructures
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks that do occur.

According to the National Strategy to Secure Cyberspace, the private sector is best equipped and structured to respond to an evolving cyber threat.[21] The government plans to protect its own network and the private sector critical infrastructure essential missions and services. The government has five national priorities/programs in which they fill a role to secure cyberspace. The priorities/programs are:

- A National Cyberspace Security Response System
- A National Cyberspace Security Threat and Vulnerability Reduction Program
- A National Cyberspace Security Awareness and Training Program
- Securing Government's Cyberspace
- National Security and International Cyberspace Security Cooperation.[22]

The first priority, which focuses on improving our response and reducing the potential damage from cyber incidents, does not include a military response or any type government demarche to denounce any such intrusion. The nation's policy stresses protection of information systems for critical infrastructures, which helps to protect the people, economy, and national security of the United States.[23] There is a huge emphasis on partnering with the private sector, inviting the private sector to create an organization to make U.S. cyberspace secure. There was no mention of a cyber deterrence posture in the national policy. If the U.S. were successful in collaborating with the international community, then all countries would support the same cyber norms, therefore, no need to have a cyber deterrence posture.

LAW ENFORCEMENT

Cyber incidents and intrusions have been occurring for some time, but despite that, the international community has not defined cyber warfare or agreed on international norms for cyberspace. The current international law is undeveloped and maladapted to define cyber warfare. The Council of Europe has defined cyber intrusions and aggression as a crime. The forty-one nation Council of Europe (COE) drafted the Cybercrime Convention after four years and twenty-seven drafts. The Committee of Ministers adopted it during the Committee's 109th Session on November 8, 2001.[24]

Currently the Federal Bureau of Investigations (FBI), which is part of the Department of Justice, has jurisdiction over cyber incidents, which include cyber intrusions, cyber espionage, and denial of service attacks. However, DoD has primary responsibility to defend U.S. cyberspace during acts of war against the U.S. homeland or interests abroad. It is the responsibility of the FBI to determine whether a cyber incident is or is not an act of war. Initially, cyber incidents are ambiguous and their intent is uncertain. Determining where attacks originated, why the attacker initiated the attack, and who is responsible, is difficult and it does not happen very fast. Sometimes organizations never identify the origin or the sponsor of the attack.

The FBI and other law enforcement agencies are responsible for determining if the intent of the attack was an act of war because the international community has not defined cyberwarfare. Although investigations of cyber attacks are difficult and time consuming, the FBI has proven technology, techniques, and procedures to hunt down and capture cyber criminals, despite the anonymity of the internet. The FBI conducts theses tasks through partnership initiatives with the private sector as described in the National Strategy to Defend Cyberspace document.

The FBI has Cyber Action Teams that travel around the world on a moment's notice to respond to cyber intrusions. Along the way, they gather vital intelligence on emerging threats and trends that help identify cyber crimes that are most dangerous to U.S. security and economy. The FBI is actively part of Computer Crimes Task Force, National Cyber Investigative Joint Task Force, National Cyber-Forensics and Training Alliance, Strategic Alliance Cyber Crime Working Group and Infragard. These organizations are comprised of the private sector and international partners to help stop cyber crime and make it harder for cyber criminals to commit crime on the internet.

MILITARY

The U.S. military relies on DoD information network to conduct business and to wage war, but the DoD information network relies on the backbone of U.S. networks.

Large internet providers such as Level 3 Communications, Verizon, Sprint, Qwest, and Deutsche Telekom operate the backbone of the internet. The DoD information network connects into the backbone to access the internet and DoD's classified network connects by riding over the backbone. If there were any degradation in the U.S. backbone network, it would affect DoD information network too. While DoD depends on the Department of Homeland Security (DHS) to keep the backbone network secure, DoD has to defend against viruses, malicious codes, and intrusions that directly affect the DoD information networks.

Over the past decade the frequency and sophistication of intrusions into government networks has increased exponentially[25]. Malicious actors probe and scan Government, DoD, and contractor networks over a million times per day[26]. The U.S. Department of Defense (DoD) suffered a significant compromise of its classified military computer networks in 2008. This classified incident was the most significant breach of U.S. military computers ever. Hackers exploited the vulnerabilities in three contractor networks to steal intellectual property relating to the Joint Strike Fighter project, a 300 billion dollar DoD project. The hackers stole several terabytes of data, which could make it easier to defend against the Joint Fighter. Wall Street Journal reports that the hackers were not able to download the most sensitive material, which is stored on computers not connected to the internet.[27]

According to Wall Street Journal, cyber spies penetrated and gained access to the Supervisory Control and Data Acquisition systems that control the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials[28]. The Wall Street Journal reports Russian and Chinese cyber spies were studying and mapping the electrical grid with no intent to cause damage to the electrical grid. However, authorities have found software left behind that could destroy electric grid infrastructure components, which could be, used in future conflicts with Russia or China.[29]

Following these attacks the dual-hatted Commander of JFCC-NW and Director of National Security Agency (NSA) realized that the military needed a new approach for cyber operations. He lobbied to combine JFCC-NW and JTF-GNO to create the United States Cyber Command (USCYBERCOM) in order to plan, coordinate, integrate, and synchronize offensive operations and defensive operations and daily Network Operations (NetOps) for military networks.

USCYBERCOM

JTF-GNO, activated in 1998 as a subordinate command to United States Strategic Command (USSTRATCOM), directed the operation and defense of the DoD information networks across strategic, operational, and tactical boundaries. JFCC-NW, also a subordinate component command of USSTRATCOM, started operations in 2005. JFCC-NW led and coordinated computer network attack operations for DoD with national and international organizations to protect government, private sector and Allied partner computer networks. The NSA directed and conducted enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks, defined as Computer Network Exploitation (CNE).

On 23 June 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish a sub-unified command to plan, coordinate, integrate, synchronize, direct, and conduct activities to operate and defend the Department of Defense information networks. U.S. Cyber Command (USCYBERCOM) started initial operations on 21 May 2010[30]. USCYBERCOM assumed the day-to-day Computer Network Defense (CND) and Computer Network Attack (CNA) operations for two organizations, the Joint Task Force for Global Network Operations (JTF-GNO) and the Joint Functional Component Command for Network Warfare (JFCC-NW). NSA retained day to day Computer Network Exploitation (CNE) operations, which enables intelligence gathering and is an activity executed under authorities granted in Title 50, U.S. code. USCYBERCOM does not have the legal authorities granted under Title 50 U.S. Code to conduct CNE; therefore, NSA continues the directing and conducting CNE.

USCYBERCOM, which is co-located with NSA and commanded by the same leader, centralizes command of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise. Combining the two organizations allows USCYBERCOM to view the full cyber Common Operational Picture (COP) and the integration allows offensive and defensive operations to share information more effectively and efficiently. As defensive operations encounter new viruses and methods that hackers are using, they share it with offensive operations for their use. Offensive operations do the same for defensive operations; they pass new attack methods to defensive operations so that they can defend against them. Consequently, USCYBERCOM improves DoD's capabilities to ensure resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace.

USCYBERCOM’s efforts support the Armed Services’ ability to confidently conduct high-tempo, effective operations as well as protect command and control systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions and attacks.[31] In order to support USCYBERCOM, the services consolidated their individual cyber forces and activated cyber components. DoD is training and equipping cyber security experts and expects to develop a readily available workforce of cyber specialists.

There are at least 13 different doctrinal documents at the Office of the Secretary of Defense (OSD), DoD, agency, Service, and USSTRATCOM levels that outline how DoD will fight a cyber war[32]. DoD must continue consolidating authorities, organizations and doctrinal documents to improve their speed of command, share information and execute missions in cyberspace. Cyber operations are scattered and fragmented across the Services and agencies. The Services, Defense Information Systems Agency (DISA), National Security Agency (NSA), Intelligence Community, and the other Combatant Commands have unsynchronized cyberspace warfighting capabilities[33]. The services remain responsible for day-to-day defense of the networks. DISA operates and sustains the enterprise infrastructure, information sharing services, and enables command and control. DISA delivers end-to-end enterprise-wide systems engineering for the DoD information networks and testing to ensure joint interoperability. NSA has capabilities, expertise, and authorities to conduct signal intelligence operations missions under Title 50 authority and USCYBERCOM does not have the authority or the capability to execute these missions.

USCYBERCOM requires the latest technology and software in order to execute their computer network operations effectively. However, the acquisition process to acquire hardware, firmware, or software does not work effectively. USCYBERCOM works with the Services to develop software tools needed for computer network operations, however the Services are not obligated to develop software for USCYBERCOM. The Services will develop the software if it benefits their service and they can develop an application to use the software. Acquisition authority similar to USSOCOM's authority would allow USCYBERCOM to build or acquire software in a timely manner.

RECOMMENDATION

The United States has a daunting challenge to secure U.S. cyberspace and there are no magical software tools to secure cyberspace. To proactively protect and make U.S. cyberspace more secure, the U.S. should execute the following recommendations.

- The National Strategy to Secure Cyberspace provides good strategy and guidance, but the document is eight years old now and needs updating.
- The federal government should continue working with the private sector to secure and defend U.S. cyberspace by implementing the Disruption Tolerant Network. The U.S. should also present the protocol along with standards to the international community for implementation internationally.
- The federal government and the private sector must design an application that identifies individuals on the internet. The task will be very hard to do, mainly because users enjoy the anonymity on the internet. However, the internet will be a

safer place if law enforcers can identify individuals conducting criminal activities on the internet.

- DoD organized defensive and offensive cyber organizations under one command, USCYBERCOM. The next step is to make USCYBERCOM a unified command. DoD should give Title 50 authority to USCYBERCOM to allow them to conduct exploit operations currently executed by National Security Agency. DoD should also give USCYBERCOM acquisition authority like USSOCOM to allow USCYBERCOM to develop, build or buy software tools necessary for cyber operations.
- Department of Homeland Security, Department of Justice and Department of Defense must develop technology, policy, and processes to conduct proactive operations to defend U.S. cyberspace. One of the organizations needs to conduct proactive operations to guard internet access points that connects U.S. cyberspace to the international community. Another organization needs to secure and monitor cyberspace internal to the borders of U.S. cyberspace.
- The U.S. must continue to work actively in international organizations, establish cyber norms, and convince China and Russia to sign and support the Council of Europe Cyber Crime Convention. The international community needs to establish cyber norms. The international community needs to establish policies and processes for attacks originating in one country and attacking another. Cyber criminals are using servers and proxies in one country to execute their criminal activities in another country and the international community needs to develop processes for the originating country and attacked country to mitigate these attacks.

- Collaborate with industry to develop technology to identified malicious code on all electronic products. This technology will prevent malicious actors from gaining access through software code that allows access remotely or allows a malicious actor to shut down your system remotely.
- Continue researching security issues dealing with IPv6. Develop standards, processes, and policies for the secure implementation of IPv6. Share those processes, policies and standards with the international community for their implementation
- The federal government needs to form a council to govern the security standards and policies for new technology.
- Update and refine the U.S. plan to promote a comprehensive national awareness program
- Update and refine the Nation's training and education programs to support the Nation's cyber security needs.

In this early hour, the United States' greatest strength is its awareness of vulnerabilities on the network. To change the strength to proactive defense of the network, the United States must develop tools, procedures, and policies in order to defend U.S. cyberspace. The above recommendations enable the federal government to start creating tools, procedures, and policies that builds a proactive defense to secure U.S. cyberspace.

CONCLUSION

The United States is a nation fully dependent on cyberspace and that fact will not change in the future. The private sector and the government are integrating more and more products with cyberspace to control processes through the internet. Manufacturers, schools, universities, utility companies, and the financial sector have moved control of essential processes to cyberspace, as a result, the cost of doing business dropped and productivity sharply increased. However, cyber intrusions are threatening to raise the cost of doing business through cyberspace.[34]

The previously stated recommendations would make U.S. cyberspace a more secure environment. The United States should implement a policy to require identification to gain access into the web sites of the critical infrastructure and key resources. Identity management on critical infrastructure and key resource websites could decrease the number of attacks on those particular websites. To assist with identity management, the U.S. and the international community should replace the network centric protocols with a data centric protocol such as the Data Tolerant Network protocol. Certainly, there will be security challenges but not to the level of IPv4 or IPv6, both network centric protocols.

The federal government published the National Strategy to Secure Cyberspace in 2003. The federal government needs to update the guidance and publish another National Strategy to Secure Cyberspace. The updated strategy should provide new guidance on private sector organizations. The strategy should update the role of the newest sub-unified military command, USCYBERCOM.

DHS is the focal point for security of U.S. Cyberspace, but two other organizations have authorities to secure and defend U.S. cyberspace too. DHS, DoD, and Department of Justice (DoJ) should develop a common operational picture in which to share data and each organization would have better situational awareness of the incidents in U.S. cyberspace. A common operational picture would make it easier for DoD to pass the mission to the FBI and allow them to take lead with no delay.

The FBI is the agency with jurisdiction over cyber incidents, which include cyber intrusions, cyber espionage, and denial of service attacks in the United States. The FBI has jurisdiction because the Council of Europe Convention on Cybercrime as designated all cyber incidents as criminal activity. The United States signed and supports the convention; therefore, FBI handles all cyber incidents that occur in U.S. cyberspace as a criminal activity. The United States was correct to support the Council of Europe Convention on Cybercrime because it allows the State Department to start partnership initiatives with other countries. Supporting the convention on cybercrime also demonstrates that the U.S. is willing to work with other countries to solve the problem of computer intrusions and achieve the goal of designing a real time International Watch and Warning Threat information network.

Adversaries and malicious actors are developing offensive cyber capabilities and offense has the advantage in cyberspace. Adversaries attack through vulnerabilities in the network and software. The attacks and intrusions happen very fast and on occasions when an organization identifies an anomaly on the network, present technology cannot instantly identify the culprit behind the act. IPv4 and IPv6 are network centric protocols built for sharing information. Identity and security management were not priorities The U.S. should continue pursuing technology to secure cyberspace with new protocols such as Disruption Tolerant Network. Public and private partnership will achieve security in U.S. cyberspace. Only by acting together can we build a more secure cyberspace.

Endnotes

[1] George W. Bush, The National Strategy to Secure Cyberspace, (Washington, DC: The White House, February 2003), Executive Summary p.ix

[2]Ibid.

[3] Michael Chertoff, National Infrastructure Protection Plan, (Washington DC: Department of Homeland Defense, 2009), p.16

[4] Ibid., 1

[5] Donald Rumsfeld, National Military Strategy For Cyberspace Operations, (Washington DC: Department of Defense, December 2006), p.2, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 12 Jan 11)

[6]Vernon Loeb, "NSA Adviser Says Cyber-Assaults On Pentagon Persist With Few Clues" Washington Post, May 6, 2001, http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A51965-2001May6 (Accessed Feb 19, 2011) .

[7] Sean Convery, Darrin Miller, Cisco White Paper, IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)

[8] Bruce D. Caulkins, " Proactive Self-Defense in Cyberspace," The Land Warfare Papers No.72, August 2009, p.10

[9] Ibid.

[10] Jacob West, " The Quantum Computer", April 28, 2000 http://www.cs.rice.edu/~taha/teaching/05F/210/news/2005_09_16.htm (accessed 26 Jan 11)

[11] Ibid.

[12] John Markoff, "Quantum Computing Reaches For True Power," The New York Times, http://www.nytimes.com/2010/11/09/science/09compute.html (accessed 26 Jan 11)

[13] Ibid.

[14] William F. Lynn III., "Defending a New Domain: The Pentagon's New Cyberstrategy" Foreign Affairs, September/October 2010: Page 97.

[15] Ibid., 101.

[16] Dennis C. Blair,, "Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence," http://www.dni.gov/testimonies/20090212_testimony.pdf (accessed 10 Jan 11), p.39

[17] William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," Foreign Affairs 89, no.5 (September/October 2010): p.100

[18] George W. Bush, The National Strategy to Secure Cyberspace, (Washington, DC: The White House, February 2003), p.50

[19] Ibid., 51.

[20] Ibid., Foreword.

[21] Ibid., ix.

[22] Ibid., 51.

[23] Ibid., Foreword.

[24] Mike Keyser, “The Council of Europe Convention on Cybercrime” p.296

[25] William F. Lynn III., “Defending a New Domain: The Pentagon’s New Cyberstrategy” Foreign Affairs, September/October 2010: Page 97.

[26] Ibid., 100.

[27] Siobhan Gorman, August Cole and Yochi Dreazen, “Computer Spies Breach Fighter-Jet Project,” April 21, 2009, http://online.wsj.com/article/SB124027491029837401.html (accessed Dec 1, 2010).

[28] Siobhan Gorman, “Electricity Grid Penetrated by Spies”, April 8, 2009, http://online.wsj.com/article/SB123914805204099085.html (accessed Feb 12, 2011)

[29] Ibid.

[30] The United States Strategic Command Home Page, http://www.stratcom.mil/factsheets/Cyber_Command/ (Accessed Dec 3, 2011)

[31] Ibid.

[32] David Hollis, “The Need For A Unified Command” Joint Force Quarterly, / issue 58, 3d Quarter 2010, http://www.ndu.edu/press/lib/images/jfq-58/JFQ58_48-53_Hollis.pdf (accessed 18 Jan11)

[33] Ibid.

[34] George W. Bush, The National Strategy to Secure Cyberspace, (Washington, DC: The White House, February 2003), Executive Summary p.5